Coss 1-1-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: ________________ Date: December 6, 2005

Applicant(s):	M.J. Coss et al.
Case:	1-1-1
Serial No.:	08/927,382
Filing Date:	September 12, 1997
Group:	2131
Examiner:	Christopher A. Revak
Title:	Methods and Apparatus for a Computer Network Firewall with Multiple Domain Support

TRANSMITTAL OF REPLY BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith are the following documents relating to the above-identified patent application:

(1) Reply Brief.

It is believed that there is no additional fee due in conjunction with the response. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Ryan, Mason & Lewis, LLP Deposit Account No. 50-0762** as required to correct the error.

Respectfully submitted,

William E Lewis

Date: December 6, 2005

William E. Lewis
Reg. No. 39,274
Attorney for Applicant(s)
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946

AF
IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s):	M.J. Coss et al.
Case:	1-1-1
Serial No.:	08/927,382
Filing Date:	September 12, 1997
Group:	2131
Examiner:	Christopher A. Revak

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature: ______________ Date: December 6, 2005

Title: Methods and Apparatus for a Computer Network Firewall with Multiple Domain Support

---

REPLY BRIEF

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Applicants (hereinafter referred to as "Appellants") submit this Reply Brief under 37 C.F.R. §1.193(b)(1) in response to the Examiner's Answer mailed on October 6, 2005 relating to the Appeal Brief filed on July 11, 2005 appealing the final rejection of claims 1-26 of the above-identified application.

ARGUMENT

In the Examiner's Answer, the Examiner reiterates that claims 1-26 are anticipated under 35 U.S.C. §102(e) based on U.S. Patent No. 5,835,726 to Shwed et al. (hereinafter Shwed '726), and unpatentable under 35 U.S.C. §103(a) based on U.S. Patent No. 5,606,668 to Shwed et al. (hereinafter Shwed '668). The Examiner, in section (10) of the Examiner's Answer, presents further arguments in support of such rejections. Appellants will respectively address below the further arguments offered in the Examiner's Answer. Nonetheless, Appellants re-allege herein and incorporate by reference the arguments presented in the Appeal Brief dated July 11, 2005 in their entirety.

Please note that the sections to follow correspond to the sub-sections in section (10) of the Examiner's Answer.

A(I). The Examiner states at page 4 of the Examiner's Answer:

> The teachings of Shwed '726 disclose receiving a packet where control passes to block 410 in which code is generated to match the rule services that were chosen, or selected, and the rule services have been previously defined and a decision is then made as to whether to accept or reject the packet based on the security rule, see column 8, lines 19-33. The citation of Shwed recites that the given policy is pre-selected and that the rule services are based on filter scripts that contain the rules used by the packet filter, see column 8, lines 10-14.

Appellants respectfully point out that the Examiner's Answer is confusing two separate operations disclosed in Shwed '726, namely, packet filter generation and packet filtering. FIG. 4 of Shwed (referred to above) describes the subsystem for converting graphical information to a filter script, i.e., packet filter generation, see column 4, lines 51-52. That is, FIG. 4 illustrates how a network administrator may specify different security rule sets for different business entities in accordance with a GUI-based subsystem. As clearly further explained at column 6, lines 42-45, the rule set specified by the network administrator is then processed by the packet filter generator and the resulting code is transmitted to the appropriate packet filter in the network.

However, this is clearly distinct from actually filtering a packet using the resulting code upon receipt of a packet. As clearly further explained at column 9, lines 18-50, a packet entering the computer, at a particular connection, on which the generated packet filter resides is diverted to the packet filter, wherein the associated single rule set is applied to validate the packet.

Again, it seems that the Examiner's Answer confuses the network administrator determining what rule set to put on the firewall at the time of packet filter generation, with the firewall applying the single rule set at the time a packet is received.

Therefore, unlike the claimed invention, there are no steps in Shwed '726 performed by the firewall that, upon receipt of a packet to be validated, first selects a security policy from among a plurality of security policies and then applies the rules associated with that particular policy. Shwed merely discloses applying a rule from the single rule set associated with the packet filter residing on that computer. In fact, Shwed '726 confirms this at column 2, lines 1-4, wherein it is stated that a computer merely applies a given security policy to a packet. That is, in Shwed, the computer does not select a security policy from among a plurality of security policies, as in the claimed invention.

A(II). Firstly, the Examiner alleges that "the claim requirement only requires selection of a, or one, security policy to meet the claim requirement.

This is not accurate. Independent claims 1, 17 and 22 recite "selecting at least one of a plurality of security policies as a function of the session key (data item), wherein a security policy comprises multiple rules, and using the selected at least one of the security policies in validating said packet." Independent claims 8 and 12 recite "designating a plurality of independent security policies, wherein a security policy comprises multiple rules, determining which security policy is appropriate for the packet, and validating the packet using at least a portion of the multiple rules of the determined security policy."

Thus, independent claims 1, 17 and 22 expressly recite selecting at least one of a plurality of security policies and independent claims 8 and 12 expressly recite designating a plurality of independent security policies . . . [and] determining which security policy is appropriate for the packet.

While Shwed uses one security policy in a packet filter, unlike the claimed invention, a Shwed packet filter never selects a security policy from among a plurality of security policies, nor does a Shwed packet filter determine which security policy among a plurality of independent security policies is appropriate for the packet.

Secondly, the Examiner again refers to the description of FIG. 4 of Shwed at column 8, lines 19-33, and alleges that this is the same as a packet filter selecting a policy from among a plurality of policies. However, for the reasons given above (section A(I)), this is incorrect. FIG. 4 of Shwed explains how a network administrator generates each rule set. Thus, while a network administrator may select which policy to place on a node, the firewall itself does not perform this selection. The Shwed firewall only implements the single policy that resides thereon, as decided by the network administrator.

Thirdly, the Examiner's Answer cites the previous Appeal Decision with regard to the distinction between multiple security rules multiple security policies. However, this is one reason why Appellants amended the independent claims to further express the distinction between multiple security rules and multiple security policies, i.e., a security policy comprises multiple rules.

A(III). Independent claim 16 recites "segmenting a plurality of security policies into a plurality of domains, wherein a domain comprises at least one security policy and a security policy comprises multiple rules, and further wherein a plurality of administrators are associated with the plurality of domains, and administering the multiple rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain."

The Examiner's Answer at page 5 refers to system operators and administrators being allowed to have flexibility in managing communications, citing column 6, line 65, through column 7, line 16. However, it is unclear to Appellants how this teaches or suggests the express claim language of independent claim 16. Such portions of Shwed are silent to the claimed features.

B(I). The Examiner seems to raise no new points in this section, but rather appears to repeat the same argument made in section A(II) of the Examiner's Answer. Thus, Appellants re-allege herein and incorporate by reference the arguments given above with respect to section A(II).

B(II). The Examiner seems to raise no new points (with one exception addressed below) in this section, but rather appears to repeat the same argument made in section A(II) of the Examiner's Answer. Thus, Appellants re-allege herein and incorporate by reference the arguments given above with respect to section A(II).

The Examiner does mention for the first time that Shwed discloses encryption of communications between two parties based on a session key and that the parties exchange this session key prior to communications. However, Appellants are unclear how this has anything to do with security policy selection in the firewall, and thus the language of the claimed invention.

B(III). The Examiner seems to raise no new points in this section, but rather appears to repeat the same argument made in section A(III) of the Examiner's Answer. Thus, Appellants re-allege herein and incorporate by reference the arguments given above with respect to section A(III).

B(IV). In their Appeal Brief dated July 11, 2005, Appellants explained how Shwed '668 suffers from the same deficiencies as Shwed '726. Thus, the Examiner seems to raise no new points in this section with respect to Shwed '668, but rather appears to repeat the same argument made in section A(II) of the Examiner's Answer with respect to Shwed '726. Thus, Appellants re-allege herein and incorporate by reference the arguments given above with respect to section A(II).

B(V). In their Appeal Brief dated July 11, 2005, Appellants explained how Shwed '668 suffers from the same deficiencies as Shwed '726. Thus, the Examiner seems to raise no new points in this section with respect to Shwed '668, but rather appears to repeat the same argument made in section A(III) of the Examiner's Answer with respect to Shwed '726. Thus, Appellants re-allege herein and incorporate by reference the arguments given above with respect to section A(III).

B(VI). Appellants re-allege herein and incorporate by reference the arguments presented in their Appeal Brief dated July 11, 2005 with respect to the session key feature. Appellants assert that the arguments therein address the final rejection upon which appeal was taken and, therefore, are appropriate.

Lastly, Appellants assert that the Examiner is absolutely wrong in asserting, at the bottom of page 11 through the top of page 12 of the Examiner's Answer, that "the matter of issues now reside in the fact of whether or not Shwed '726 and Shwed '668 disclose a 'security policy comprises multiple rules" and "a domain comprises at least one security policy and a security policy comprises multiple rules, and that a plurality of administrators are associated with the plurality of domains."

Appellants respectfully assert that the claim amendments made after the Appeal Decision where made to further clarify the distinction between security rules and security policies such that the novel concept of automated policy selection from among a plurality of security policies in a firewall was further clarified. As such, Appellants respectfully assert that the entire claim set must be re-evaluated by the Board in view of the further definition given to the distinction between security rules and security policies in the claims, which has not yet been adjudicated.

For at least the reasons given above, and given in the Appeal Brief dated July 11, 2005, Appellants respectfully request withdrawal of the §102(e) and §103(a) rejections of claims 1-26.

Respectfully submitted,

William E Lewis

Date: December 6, 2005

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946